IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

KIMBERLY BARNES, DEVON REID, AMANDA COMONOTE, MICHAEL LEWIS, CRYSTAL BIGGS, BRET GLIDEWELL, JOSEPH COOK, and DAVID CURTO, individually, and on behalf of all others similarly situated, *Plaintiffs,* v. **CAPITAL ONE FINANCIAL CORPORATION; CAPITAL ONE, N.A.,** and **CAPITAL ONE BANK (USA); N.A.** *Defendants.*	Civil Action No.: 1:19-cv-1021 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

COMPLAINT

COMES NOW, Plaintiffs Kimberly Barnes, Devon Reid, Amanda Comonote, Michael Lewis, Crystal Biggs, Bret Glidewell, Joseph Cook, and David Curto, individually, and on behalf of all others similarly situated, (collectively "Class and Subclass Members" as more fully defined below) by and through undersigned counsel, and file this Complaint against Defendants Capital One Financial Corporation, Capital One, N.A., and Capital One Bank (USA), N.A., (collectively, "Capital One" or "Defendants"), on the grounds and in the amount set forth as follows:

INTRODUCTION

1. Plaintiffs file this class action lawsuit seeking compensatory and punitive damages, injunctive and declaratory relief, and all other remedies provided under federal, state, and common law as redress for Capital One's failure to protect its customers' private, personal, financial, and confidential information, including but not limited to, Plaintiffs' bank account numbers, transaction histories, self-reported incomes, credit scores, Social Security Numbers, names,

addresses, phone numbers, emails, dates of birth, and/or other personally identifying information (collectively, "Sensitive Information"). Specifically, Paige Thompson, 33, a resident of the State of Washington and former Amazon employee, hacked the accounts of approximately 106 million Capital One cardholders, including Plaintiffs, and illegally obtained Plaintiffs' and their Class and Subclass Members (collectively, "Plaintiffs") Sensitive Information directly and proximately because Capital One failed to protect such information against breach and unauthorized access thereto.

2. Plaintiffs bring this action and assert claims for negligence, negligence *per se*, implied breach of contract, bailment, and unjust enrichment, and, individually and on behalf of each respective state-specific subclass, the state-specific consumer protection and/or privacy laws applicable regarding the governance of the forthcoming alleged conduct.

JURISDICTION & VENUE

3. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d) because Plaintiffs reside in Alabama, the District of Columbia, Georgia, Illinois, Maryland, Mississippi, and Virginia, Defendants are Delaware corporations and maintain principal places of business and headquarter offices in the Commonwealth of Virginia for diversity purposes, the amount in controversy exceeds $5,000,000.00 exclusive of interests and costs, and more than 1,000 members comprise the putative Nationwide Class and State Subclasses, respectively.

4. This Court has personal jurisdiction over Capital One because Defendants conduct business in the Commonwealth of Virginia, own, operate, control, and maintain businesses in the Commonwealth of Virginia, target, advertise, and illicit business from Commonwealth of Virginia residents, and otherwise purposefully avail themselves of the protections this jurisdiction affords to Capital One.

5. Venue is proper pursuant to 28 U.S.C. § 1391(b) in that a substantial portion of the events giving rise to this action occurred within the Commonwealth of Virginia and this Court has personal jurisdiction over Defendants.

PARTIES

A. PLAINTIFFS

6. Plaintiff Kimberly Barnes is an adult resident and citizen of Alabama. Upon information and belief, Capital One wrongfully disclosed Plaintiff Barnes' and approximately 100 million similarly situated Class and Alabama Subclass Members' Sensitive Information.

7. Plaintiff Devon Reid is an adult resident and citizen of the District of Columbia. Upon information and belief, Capital One wrongfully disclosed Plaintiff Reid's and approximately 100 million similarly situated Class and District of Columbia Subclass Members' Sensitive Information.

8. Plaintiff Amanda Comonte is an adult resident and citizen of Georgia. Upon information and belief, Capital One wrongfully disclosed Plaintiff Comonte's and approximately 100 million similarly situated Class and Georgia Subclass Members' Sensitive Information.

9. Plaintiff Michael Lewis is an adult resident and citizen of Illinois. Upon information and belief, Capital One wrongfully disclosed Plaintiff Lewis's and approximately 100 million similarly situated Class and Illinois Subclass Members' Sensitive Information.

10. Plaintiff Joseph Cook is an adult resident and citizen of Maryland. Upon information and belief, Capital One wrongfully disclosed Plaintiff Cook's and approximately 100 million similarly situated Class and Maryland Subclass Members' Sensitive Information.

11. Plaintiff Crystal Biggs is an adult resident and citizen of Mississippi. Upon information and belief, Capital One wrongfully disclosed Plaintiff Biggs's and approximately 100 million similarly situated Class and Mississippi Subclass Members' Sensitive Information.

12. Plaintiff Bret Glidewell is an adult resident and citizen of North Carolina. Upon information and belief, Capital One wrongfully disclosed Plaintiff Glidewell's and approximately 100 million similarly situated Class and North Carolina Subclass Members' Sensitive Information.

13. Plaintiff David Curto is an adult resident and citizen of Virginia. Upon information and belief, Capital One wrongfully disclosed Plaintiff Curto's and approximately 100 million similarly situated Class and Virginia Subclass Members' Sensitive Information.

B. DEFENDANTS

14. Defendant Capital One Financial Corporation is a Delaware corporation and maintains its principal place of business at 1680 Capital One Drive, McClean, Virginia 22102.

15. Defendant Capital One, N.A., is a Delaware corporation and a wholly-owned subsidiary of Capital One Financial Corporation and maintains its principal place of business at 1680 Capital One Drive, McClean, Virginia 22102.

16. Defendant Capital One Bank (USA) N.A., is a national bank and a wholly-owned subsidiary of Capital One Financial Corporation and maintains its principal place of business at 1680 Capital One Drive, McClean, Virginia 22102.

FACTS

17. At all times relevant to this action, Plaintiffs applied for, and/or maintained credit cards and corresponding accounts with Capital One. In the process of applying for their credit cards, Plaintiffs divulged, without limitation, bank account numbers, transaction histories, self-reported incomes, credit scores, Social Security Numbers, names, addresses, phone numbers,

emails, dates of birth, and/or other personally identifying information (collectively, "Sensitive Information") to Capital One.

18. Defendant Capital One Financial Corporation, through its subsidiaries, including Defendants Capital One, N.A., and Capital One Bank (USA), N.A., is one of the largest credit-card issuers in the United States, and one of the top 10 largest banks based on deposits, serving approximately 45 million customer accounts.

19. On July 29, 2019, Capital One publicly announced a Data Breach and issued the following statement:

> [O]n July 19, 2019, it determined there was unauthorized access by an outside individual who obtained certain types of Sensitive Information relating to people who had applied for its credit card products and to Capital One credit card customers Based on our **analysis to date**, this event affected approximately 100 million individuals in the United States and approximately 6 million in Canada . . . [and] the largest category of information accessed was information on consumers and small businesses as of the time they applied for one of our credit card products from 2005 through early 2019.

(hereinafter, "Data Breach") (**emphasis** added).

20. Capital One further disclosed that the Data Breach further disclosed Sensitive Information including, without limitation, approximately 80,000 customers' bank account numbers and 140,000 customers' Social Security Numbers, transaction histories, self-reported incomes, credit scores, names, addresses, phone numbers, emails, dates of birth, and/or other personally identifying information.

21. On July 19, 2019, Defendants discovered the March 22-23, 2019 Data Breach and publicly disclosed the same on July 29, 2019; more four (4) months after Capital One's approximately 100 million customers and credit card applicants Sensitive Information was compromised.

22. Notwithstanding the March 22-23rd Data Breach, Defendants failed to stop the hacker or take remedial action and as a result, the hacker continued to access to Capital One's customers and applicants for another twenty-eight (28) days, until April 21, 2019.

23. Capital One failed to discover the Data Breach on its own; rather, Capital One merely discovered the information through an anonymous source that sent a link time-stamped April 21, 2019 to Capital One containing the leaked Sensitive Information via email. The link also contained the command codes used in the intrusion and more than 700 data folders.

24. Capital One promised its cardholders, applicants, and customers, such as Plaintiffs and their Class and Subclass Members, to keep their Sensitive Information confidential and to protect it from unauthorized disclosures in accord based on industry standards. Specifically, Capital One's credit card application explicitly states, "Capital One uses 256-bit Secure Sockets Layer (SSL) technology. This means that when you are on our website, the data transferred between Capital One and you is encrypted and **cannot be viewed by any other party.**"

25. Plaintiffs and their Class and Subclass Members provided their Sensitive Information to Capital One with the understanding and expectation that Capital One, affiliates, subsidiaries, and business partners to whom Capital One disclosed the Sensitive Information would comply with their obligations to keep their Sensitive Information confidential and secure from unauthorized access and/or disclosures.

26. Capital One promises customers that it will keep their Sensitive Information confidential, assuring customers on its credit card applications explicitly that

27. Defendants' failed to honor their duties and promises by not providing, using, implementing, monitoring, and/or employing adequate security features, failed to maintain an adequate data security system to reduce the risk of Data Breaches and cyber-attacks, and

adequately monitoring its system to identify Data Breaches and cyber-attacks and protect Plaintiffs' and their Class and Subclass Members' Sensitive Information, thereby causing Plaintiffs and their Class and Subclass Members' to suffer harm, damages, and pecuniary and other non-economic losses.

28. Notwithstanding the applicable industry standard, Capital One's failure to honor its obligations, both imposed and contractually required, amount to recklessness given the substantial increase hacking, breaches, and unauthorized access and dissemination of Sensitive Information. Capital One, as the top ten largest banks in the United States should be fully aware of, and able to, prevent such attacks given their posture in the cyber and financial industries.

29. Moreover, Capital One should have exercised hyper-vigilance regarding its conduct in monitoring Plaintiffs' and their Class and Subclass Members' Sensitive Information as this is not the first time Capital One has been hacked. In January of 2018, a hacker compromised approximately 50GB of Sensitive Information. In response, Capital One sent letters to its customers advising that their Sensitive Information "may have been breached[1]," however, upon information and belief and as evidenced by the Data Breach giving rise to this action, Capital One failed to take reasonable and necessary precautionary measures to prevent another breach.

30. The United States Government Accountability Office noted in a March 2019 report on Data Breaches:

> Perpetrators of fraud can use stolen Sensitive Information—such as account numbers, passwords, or Social Security numbers—to take out loans or seek medical care under someone else's name, or make unauthorized purchases on credit cards, among other crimes. Foreign state-based actors can use Sensitive Information to support espionage or other nefarious uses.

[1] This is not the first time Capital One has informed its consumers their Sensitive Information "may have been compromised." Capital One sent similar letters to its customers in November of 2014, twice in July of 2017, and again in September 2017.

Data Breaches: Range of Consumer Risks Highlights Limitations of Identity Theft Services GAO-19-230, March 2019 ("GAO Report"), at i.

31. Data stolen in the Capital One breach can be held and used years from now. The GAO stated, "Once [data] is exposed, there is no time limit on the potential for identity thieves to use such information to commit fraud." *Id*., at fn 24.

32. Although Congress and several states have enacted legislation for consumer protections and commercially-available identity theft services offer some assistance in prevention, the GAO notes private companies that hold consumer data, like Defendants, have a responsibility to protect those data. "The burden should not be on consumers to protect data they do not control." *Id*., at 14.

33. Identity theft occurs when individuals' sensitive Sensitive Information is used without authorization in an attempt to commit fraud or other crimes.

34. Harm resulting from exposure of sensitive Sensitive Information includes financial fraud (new-account fraud, existing-account fraud); tax refund fraud; government benefits fraud; and medical identity theft (which occurs when someone uses an individual's name or personal identifying information to obtain medical services or prescription drugs fraudulently, including submitting fraudulent insurance claims).

35. The federal government has identified synthetic identity theft as an emerging criminal trend. Synthetic identity theft, which involves the creation of a fictitious identity, typically by using a combination of real data and fabricated information. For example, the perpetrator steals a Social Security number and combines it with a second person's birthdate and a third person's credit card number.

36. In addition to these tangible financial losses, harm also occurs in emotional distress, reputational harm and lost time, the hours taken to obtain new identification, credit cards, and other documents. The GAO reported the time has significantly decreased, but about one percent of victims will spend six months or more resolving identity theft issues.

37. Criminals are capable of far more than retrieving funds from a victim's bank; they commit various forms of fraud, obtaining driver's licenses or official identification cards in the victim's name but with the thief's picture, use the victim's name and Social Security Number to obtain government benefits, and file fraudulent tax return using the victim's information, seek and obtain employment posing under the guise of the victim, rent and buy homes, and even cause victim's to be arrested as a result of warrants being issued in the victim's name.

38. Sensitive Information is an invaluable commodity in the current global market and once the information has been compromised, that information is sold and weaponized in the black market for years to come.

39. Data Breaches are not merely the divulgence of Sensitive Information to unauthorized viewers, but rather, a systemic problem that can be prevented. Data Breaches cripple the lives of victims and the global economy and financial institutions whom require such information should handle the same with nothing shy of the upmost vigilance.

CLASS ALLEGATIONS

40. Pursuant to FED. R. CIV. P. 23(b)(1)–(3) and (c)(4), Plaintiffs assert Capital One violated the FCRA as well as common law claims for negligence, negligence *per se*, bailment, and unjust enrichment and seek declaratory and injunctive relief, on their behalves and on behalf of the forthcoming nationwide class ("Nationwide Class") and state subclass:

NATIONWIDE CLASS DEFINED

All residents of the United States who provided, authorized, or disclosed Sensitive Information to Capital One and as a result, suffered a compromise of the aforesaid Sensitive Information as a result of a Data Breach Capital One publicly announced on or about July 29, 2019.

STATEWIDE SUBCLASSES DEFINED

All residents of the [STATE[2]] who provided, authorized, or disclosed Sensitive Information to Capital One and as a result, suffered a compromise of the aforesaid Sensitive Information as a result of a Data Breach Capital One publicly announced on or about July 29, 2019.

41. Excluded from the foregoing Class and State-Specific Statewide Subclasses are Capital One Financial Corporation, Capital One, N.A., and Capital One Bank (USA), N.A. and any other entities in which Capital One has a controlling interest, inclusive of all such entities' officers, directors, legal representatives, successors, subsidiaries, and assigns.

A. NUMEROSITY, FED. R. CIV. P. 23(a)(1)

42. The members of the Class and Subclasses are so numerous and geographically dispersed as to make joinder of all Class and each respective Subclass' members impracticable. Plaintiffs, in reliance upon Capital One's public statement[3], are informed and believe that approximately 100 million individuals in the United States have been affected by the Data Breach and the affected individuals' names and addresses are available and ascertainable based upon Capital One's records. Class members may be notified of the pendency of this action by

[2] The [STATE] shall be construed to mean each state of which Plaintiffs are citizens, including Alabama, the District of Columbia, Georgia, Illinois, Maryland, Mississippi, North Carolina, and Virginia, respectively. Notwithstanding the state-specific substitution, the Subclass Definition remains the same for each Subclass.

[3] https://www.capitalone.com/facts2019/ (last accessed August 1, 2019) "On July 19, 2019, we determined that an outside individual gained unauthorized access and obtained certain types of personal information about Capital One credit card customers and individuals who had applied for our credit card products. Based on our analysis to date, this event affected approximately **100 million individuals in the United States** and approximately 6 million in Canada." (**emphasis** added).

recognized and Court-approved notice dissemination methods, such as U.S. Mail, electronic mail, electronic/Internet postings, and/or public notices.

B. COMMONALITY, FED. R. CIV. P. 23(a)(2) and (b)(3)

43. This action involves common questions of law and fact identical to each Class and Subclass member and such common questions predominate over any questions affecting individual class members without limitation. Specifically, the common questions of law and fact include, *inter alia*:

a. Whether Capital One knew or should have known that its computer systems and electronically stored information ("ESI") were vulnerable to attack;

b. Whether Capital One failed to act reasonably and take adequate measures to ensure Plaintiffs' Sensitive Information was protected against unauthorized access;

c. Whether Capital One failed to take available precautionary steps and measures to prevent the Data Breach from ever occurring;

d. Whether Capital One failed to disclose the material facts that it did not have adequate computer systems and security practices to safeguard consumers' financial and personal data;

e. Whether Capital One failed to provide timely and adequate notice of the Data Breach;

f. Whether Capital One owed a duty to Plaintiffs and their Class and Subclass Members to protect their Sensitive Information and to provide timely and accurate notice of the Data Breach to Plaintiffs and their Class and Subclass Members;

g. Whether Capital One breached its duties to protect the Sensitive Information of Plaintiffs and their Class and Subclass Members by failing to provide adequate data security and by failing to provide timely and accurate notice to Plaintiffs and their Class and Subclass Members of the Data Breach;

h. Whether Capital One's acts and/or omissions proximately caused the Data Breach that resulted in the unauthorized access and/or dissemination of Plaintiffs' Sensitive Information;

i. Whether Capital One violated state-specific consumer protection acts;

j. Whether Capital One violated state-specific privacy laws;

k. Whether Capital One's acts and/or omissions renders Defendants liable for: (1) negligence; (2) negligence *per se*; (3) bailment; and/or (4) unjust enrichment;

l. Whether, as a result of Capital One's acts and/or omissions, Plaintiffs and Class and Subclass Members are subject to significant harm and/or have already suffered harm, and if so, the appropriate measure of damages to which Plaintiffs and Class and Subclass Members are entitled; and

m. Whether, as a result of Capital One's acts and/or omissions, Plaintiffs and Class and Subclass Members are entitled to equitable, injunctive, declaratory and/or other appropriate relief, and if so, the measure and nature of such relief.

C. TYPICALITY, FED. R. CIV. P. 23(a)(3)

44. Plaintiffs' claims are typical of their Class and Subclass Members' claims because Capital One's acts and/or omissions subjected Plaintiffs and the Class and Subclass Members to the same harm and Plaintiffs and Class and Subclass Members sustained the same damages.

D. ADEQUATE REPRESENTATION, FED. R. CIV. P. 23(a)(4)

45. Plaintiffs are adequate class representatives because their interests do not conflict with their Class and Subclass Members' interests whom Plaintiffs seeks to represent, Plaintiffs have retained counsel competent and experienced in complex class action litigation, and Plaintiffs intend to vigorously prosecute this action on behalf of all Class and Subclass Members. Class and Subclass Members' interests will be fairly and adequately protected by Plaintiffs and their counsel.

E. DECLARATORY AND INJUNCTIVE RELIEF, FED. R. CIV. P. 23(b)(2)

46. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members that would establish incompatible standards of conduct for Capital One. Such individual actions would create a risk of adjudications which would be dispositive of the interests of their Class members and impair their interests. Capital One has acted and/or refused to act on grounds generally applicable to the Class, making final injunctive relief or corresponding declaratory relief appropriate.

E. SUPERIORITY, FED. R. CIV. P. 23(b)(3)

47. A class action is superior to any other means available to fairly and efficiently adjudicate the Data Breach giving rise to this action. Plaintiffs do not anticipate any unusual difficulties in managing and maintaining this class action, and the damages and financial detriment Plaintiffs and their Class and Subclass Members suffered is comparably small to the burden and expense required and necessarily incurred by litigating each claim on an individual basis. Thus, it would be impracticable for Plaintiffs' Class and Subclass Members to individually seek redress for Capital One's identical wrongful conduct. Moreover, assuming *arguendo* each Class and Subclass Member could afford competent counsel, the Courts simply cannot. Individual litigation of potentially 100 million cases in 50 or more United States District Courts is substantially likely to yield inconsistent holdings and judgments, thereby not only affecting federal trial courts, but also flooding the United States Circuit Courts with appeals and unnecessary delay, volume, and expenses to the American judicial system. In stark contrast, the litigation of this action and permitting Plaintiffs to represent their similarly situated Class and Subclass Members alleviates the expense and burden upon the aforesaid District and Circuit Courts, and provides the benefit of consistent judgments, a single adjudication, and preserves judicial economy, as well as financially benefits all claimants harms as a result of the forthcoming allegations.

FIRST CLAIM FOR RELIEF

NEGLIGENCE

(*Asserted by all Plaintiffs and their Class and Subclass Members, respectively*)

48. Plaintiffs, individually and on behalf of all their Class and Subclass Members, repeat and reallege all preceding paragraphs as if fully set forth herein.

49. Capital One owed a duty to Plaintiffs and their Class and Subclass Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting

Plaintiffs' and their Class and Subclass Members' Sensitive Information in Capital One's possession from being compromised, lost, stolen, accessed and/or misused by unauthorized persons.

50. Capital One further owed further owed a duty to Plaintiffs and their Class and Subclass Members to implement processes that would detect a breach of its security system in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

51. Capital One further owed a duty to Plaintiffs and their Class and Subclass Members to provide security, including consistent with industry standards and requirements, to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the Sensitive Information of Plaintiffs and their Class and Subclass Members about whom Capital One collected, maintained, and used such information.

52. Capital One further owed Plaintiffs and their Class and Subclass Members the aforesaid duty(ies) because Plaintiffs and their Class and Subclass Members were foreseeable and probable victims of any inadequate security practices. Capital One solicited, gathered, and stored Plaintiffs' and their Class and Subclass Members' Sensitive Information and knew it inadequately safeguarded such Sensitive Information on its computer systems and that hackers routinely attempted to access this valuable data without authorization.

53. Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, also imposed a duty upon Capital One to use reasonable data security measures. Section 5 of the FTCA prohibits "unfair…practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect Sensitive Information by companies such as Capital One. Various FTC publications and data security breach orders

further form the basis of Capital One's duty, and individual states have even enacted statutes based upon the FTC Act to mirror the aforesaid statutory duty.

54. Capital One breached its aforesaid duty(ies) by failing to design, maintain, and test its security systems to ensure adequate security and protection.

55. Capital One knew that a breach of its systems would damage Plaintiffs and their Class and Subclass Members and had a duty to adequately protect such Sensitive Information.

56. Capital One owed a duty to timely and accurately disclose to Plaintiffs and their Class and Subclass Members that their Sensitive Information had been or was reasonably believed to have been compromised. Timely disclosure was required, appropriate and necessary so that, among other things, Plaintiffs and their Class and Subclass Members could take appropriate measures to avoid unauthorized charges to their credit or debit card accounts, cancel or change usernames and passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services and take other steps to mitigate or ameliorate the damages caused by Capital One's misconduct.

57. Plaintiffs and their Class and Subclass Members entrusted, directly and indirectly, Capital One with their Sensitive Information, on the premise and with the understanding that Capital One would safeguard their information, and Capital One was in a position to protect against the harm suffered by Plaintiffs and their Class and Subclass Members as a result of the Capital One Data Breach.

58. Capital One knew, or should have known, of the risks inherent in collecting and storing the Sensitive Information of Plaintiffs and their Class and Subclass Members and of the critical importance of providing adequate security of that information.

59. Capital One's own conduct also created a foreseeable risk of harm to Plaintiffs and their Class and Subclass Members. Capital One's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent and stop the Data Breach as set forth herein. Capital One's misconduct also included its decision not to comply with industry standards for the safekeeping and maintenance of the Sensitive Information of Plaintiffs and their Class and Subclass Members.

60. Capital One breached the duties it owed to Plaintiffs and their Class and Subclass Members by failing to exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the Sensitive Information of Plaintiffs and their Class and Subclass Members.

61. Capital One breached the duties it owed to Plaintiffs and their Class and Subclass Members by failing to properly implement technical systems or security practices that could have prevented the loss of the data at issue.

62. Capital One breached the duties it owed to Plaintiffs and their Class and Subclass Members by failing to properly maintain their Sensitive Information. Given the risk involved and the amount of data at issue, Capital One's breach of its duties was entirely unreasonable.

63. Capital One breached its duties to timely and accurately disclose that Plaintiffs and their Class and Subclass Members Sensitive Information in Capital One's possession had been or was reasonably believed to have been, stolen or compromised.

64. Capital One's failure to comply with its legal obligations and with industry standards and regulations, and the delay between the date of intrusion and the date Capital One disclosed the Data Breach, further evidence Capital One's negligence in failing to exercise

reasonable care in safeguarding and protecting Plaintiffs' and their Class and Subclass Members' Sensitive Information in Capital One's possession.

65. Capital One knew that Plaintiffs and their Class and Subclass Members were foreseeable victims of a Data Breach of its systems because of laws and statutes that require Capital One to reasonably safeguard sensitive payment information, as detailed herein.

66. But for Capital One's wrongful and negligent breach of its duties owed to Plaintiffs and their Class and Subclass Members, their Sensitive Information would not have been compromised.

67. The injury and harm suffered by Plaintiffs and their Class and Subclass Members as set forth above was the reasonably foreseeable result of Capital One's failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and their Class and Subclass Members' Sensitive Information within Capital One's possession. Capital One knew or should have known that its systems and technologies for processing, securing, safeguarding and deleting Plaintiffs' and their Class and Subclass Members' Sensitive Information were inadequate and vulnerable to being breached by hackers.

68. Plaintiffs and their Class and Subclass Members suffered injuries and losses described herein as a direct and proximate result of Capital One's conduct resulting in the Data Breach, including Capital One's lack of adequate reasonable and industry standard security measures. Had Capital One implemented such adequate and reasonable security measures, Plaintiffs and their Class and Subclass Members would not have suffered the injuries alleged, as the Capital One Data Breach would likely have not occurred.

69. As a direct and proximate result of Capital One's negligent conduct, Plaintiffs and their Class and Subclass Members have suffered injury and the significant risk of harm in the future and are entitled to damages in an amount to be proven at trial.

WHEREFORE, Capital One is liable to Plaintiffs and their Class and Subclass Members for any actual damages in an amount in excess of $75,000.00 and in a sum certain amount to be determined at trial, punitive damages in an amount to be determined at trial, as well as reasonable attorney's fees, costs, and any other relief this Honorable Court deems just and proper.

SECOND CAUSE OF ACTION

NEGLIGENCE *PER SE*

(*Asserted by all Plaintiffs and their Class and Subclass Members, respectively*)

70. Plaintiff, individually and on behalf of all their Class and Subclass Members, repeats and realleges all preceding paragraphs as if fully set forth herein.

71. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair…practices in or affecting commerce" including, as interpreted and enforced by the Federal Trade Commission ("FTC"), the unfair act or practice by companies such as Capital One of failing to use reasonable measures to protect Sensitive Information. Various FTC publications and orders also form the basis of Capital One's duty.

72. Capital One violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Sensitive Information and not complying with industry standards. Capital One's conduct was particularly unreasonable given the nature and amount of Sensitive Information it obtained and stored and the foreseeable consequences of a Data Breach.

73. Capital One's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

74. The Class and Subclasses are within the class(es) of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect as they are engaged in trade and commerce and bear primary responsibility for reimbursing consumers for fraud losses. Plaintiffs and absent class members are consumers.

75. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and their Class and Subclass Members.

76. As a direct and proximate result of Capital One's negligence *per se*, Plaintiffs and their Class and Subclass Members have suffered and continue to suffer injury, including but not limited to:

a. unauthorized charges on their debit and credit card accounts;

b. theft of their Sensitive Information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;

e. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Capital One Data Breach;

f. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their credit card and Sensitive Information being placed in the hands of criminals and already misused via the sale of Plaintiffs' and Class members' information on the Internet card black market;

g. damages to and diminution in value of their Sensitive Information entrusted to Capital One with the mutual understanding that Capital One would safeguard Plaintiffs' and Class members' data against theft and not allow access and misuse of their data by others; and

h. continued risk to their financial and Sensitive Information, which remains in Capital One's possession and is subject to further breaches so long as Capital One fails to undertake appropriate and adequate measures to protect Plaintiffs.

WHEREFORE, Capital One is liable to Plaintiffs and their Class and Subclass Members for any actual damages in an amount in excess of $75,000.00 and in a sum certain amount to be determined at trial, punitive damages in an amount to be determined at trial, as well as reasonable attorney's fees, costs, and any other relief this Honorable Court deems just and proper.

THIRD CLAIM FOR RELIEF

BREACH OF IMPLIED CONTRACT

(*Asserted by all Plaintiffs and their Class and Subclass Members, respectively*)

77. Plaintiffs, individually and on behalf of all their Class and Subclass Members, repeat and reallege all preceding paragraphs as if fully set forth herein.

78. Capital One solicited and invited Plaintiffs and their Class and Subclass Members to apply for credit card products by providing their Sensitive Information. Plaintiffs and their Class and Subclass Members accepted Capital One's offers and provided their Sensitive Information to Capital One to apply for Capital One credit card products.

79. When Plaintiffs and their Class and Subclass Members applied Capital One credit card products, they provided their Sensitive Information to Capital One. In so doing, Plaintiffs and their Class and Subclass Members on the one hand, and Capital One on the other, entered into mutually agreed-upon implied contracts pursuant to which Plaintiffs and their Class and Subclass

Members agreed that their Sensitive Information was valid, while Capital One agreed that it would use Plaintiffs and Class members' Sensitive Information in its possession for the agreed-upon purpose of processing the credit card product application.

80. Implicit in the agreement to use the Sensitive Information in its possession for only the agreed-upon application and no other purpose was the obligation that Capital One would use reasonable measures to safeguard and protect the Sensitive Information of Plaintiffs and their Class and Subclass Members in its possession

81. By accepting Sensitive Information for credit card product applications, Capital One assented to and confirmed its agreement to reasonably safeguard and protect Plaintiffs' and Class members' Sensitive Information from unauthorized disclosure or uses and to timely and accurately notify Plaintiffs and their Class and Subclass Members if their data had been breached and/or compromised.

82. Plaintiffs and their Class and Subclass Members would not have provided and entrusted their Sensitive Information to Capital One to apply for the Capital One credit card products in the absence of the implied contract between them and Capital One.

83. Plaintiffs and their Class and Subclass Members fully performed their obligations under the implied contracts with Capital One.

84. Capital One breached the implied contracts it made with Plaintiffs and their Class and Subclass Members by failing to safeguard and protect Plaintiffs' and their Class and Subclass Members' Sensitive Information, and by failing to provide timely and accurate notice to them that their Sensitive Information was compromised as a result of the Data Breach.

85. Capital One breached the implied contracts it made with Plaintiffs and their Class and Subclass Members by failing to ensure that Plaintiffs' and their Class and Subclass Members'

Sensitive Information in its possession was used only for the agreed-upon application verification and no other purpose.

86. Plaintiffs and their Class and Subclass Members conferred a monetary benefit on Capital One which has accepted or retained that benefit. Specifically, the credit card products typically carry annual fees and other charges (e.g. interest) for use. In exchange, Plaintiffs and their Class and Subclass Members should have received the services that were the subject of the transaction and should have been entitled to have Capital One protect their Sensitive Information with adequate data security measures.

87. Capital One failed to secure Plaintiffs and Class members' Sensitive Information and, therefore, did not provide full compensation for the benefit Plaintiffs and their Class and Subclass Members provided.

88. Capital One acquired the Sensitive Information through inequitable means when it failed to disclose the inadequate security practices previously alleged.

89. If Plaintiffs and their Class and Subclass Members had known that Capital One would employ inadequate security measures to safeguard Sensitive Information, they would not have applied for the Capital One credit card products.

90. As a direct and proximate result of Capital One's breaches of the implied contracts between Capital One on the one hand, and Plaintiffs and their Class and Subclass Members on the other, Plaintiffs and their Class and Subclass Members have been injured as described in detail above.

91. Plaintiffs and their Class and Subclass Members were harmed as the result of Capital One's breach of the implied contracts because their Sensitive Information was compromised, placing them at a greater risk of identity theft and subjecting them to identity theft,

and their Sensitive Information was disclosed to third parties without their consent. Plaintiffs and their Class and Subclass Members also suffered diminution in value of their Sensitive Information in that it is now easily available to hackers on the dark web. Plaintiffs and their Class and Subclass Members have also suffered consequential out of-pocket losses for procuring credit freeze or protection services, identity theft monitoring, late fees, bank fees, and other expenses relating to identity theft losses or protective measures. The Class members are further damaged as their Sensitive Information remains in the hands of those who obtained it without their consent.

92. This breach of implied contracts was a direct and legal cause of the injuries and damages to Plaintiffs and Class members as described above.

WHEREFORE, Capital One is liable to Plaintiffs and their Class and Subclass Members for any actual damages in an amount in excess of $75,000.00 and in a sum certain amount to be determined at trial, punitive damages in an amount to be determined at trial, as well as reasonable attorney's fees, costs, and any other relief this Honorable Court deems just and proper.

FOURTH CLAIM FOR RELIEF

BAILMENT

(*Asserted by all Plaintiffs and their Class and Subclass Members, respectively*)

93. Plaintiff, individually and on behalf of all their Class and Subclass Members, repeats and realleges all preceding paragraphs as if fully set forth herein.

94. Plaintiffs and their Class and Subclass Members provided, or authorized disclosure of, their Sensitive Information to Capital One for the exclusive purpose of Capital One's review of credit card applications.

95. In allowing their Sensitive Information to be made available to Capital One, Plaintiffs and their Class and Subclass Members intended and understood that Capital One would adequately safeguard their Sensitive Information.

96. Capital One accepted possession of Plaintiffs' and their Class and Subclass Members' Sensitive Information for the purpose of making available to Plaintiffs and their Class members Capital One's services for their benefit.

97. By accepting possession of Plaintiffs' and their and Subclass Members' Sensitive Information, Capital One understood that Plaintiffs and their Class and Subclass Members expected Capital One to adequately safeguard their Sensitive Information. Accordingly, a bailment (or deposit) was established for the mutual benefit of the parties. During the bailment (or deposit), Capital One owed a duty to Plaintiffs and their Class and Subclass Members to exercise reasonable care, diligence, and prudence in protecting their Sensitive Information.

98. Capital One breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiffs' and their Class and Subclass Members' Sensitive Information, resulting in the unlawful and unauthorized access to and misuse of Plaintiffs' and their Class and Subclass Members' Sensitive Information.

99. Capital One further breached its duty to safeguard Plaintiffs' and their Class and Subclass Members' Sensitive Information by failing to timely and accurately notify them that their information had been compromised as a result of the Capital One Data Breach.

100. As a direct and proximate result of Capital One's breach of its duty, Plaintiffs and their Class and Subclass Members suffered consequential damages that were reasonably foreseeable to Capital One, including but not limited to the damages set forth above.

101. As a direct and proximate result of Capital One's breach of its duty, the Sensitive Information of Plaintiffs and their and Subclass Members entrusted, directly or indirectly, to Capital One during the bailment (or deposit) was damaged and its value diminished.

WHEREFORE, Capital One is liable to Plaintiffs and their Class and Subclass Members for any actual damages in an amount in excess of $75,000.00 and in a sum certain amount to be determined at trial, punitive damages in an amount to be determined at trial, as well as reasonable attorney's fees, costs, and any other relief this Honorable Court deems just and proper.

FIFTH CLAIM FOR RELIEF

UNJUST ENRICHMENT

(*Asserted by all Plaintiffs and their Class and Subclass Members, respectively*)

102. Plaintiffs, individually and on behalf of all their Class and Subclass Members, repeats and realleges all preceding paragraphs as if fully set forth herein.

103. Plaintiffs, Class members, and others conferred benefits upon Capital One in the form of sensitive information of Plaintiffs and their Class and Subclass Members, monies paid by others to access that sensitive information, and monies paid by Plaintiffs and Class members who purchased services from Capital One.

104. Capital One appreciates or has knowledge of the benefits conferred directly upon it by Plaintiffs, Class members, and others.

105. As a result of Capital One's wrongful conduct as alleged herein, Capital One has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and their Class and Subclass Members.

106. Capital One's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiffs' and their Class and Subclass Members' Sensitive Information, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

107. Under the common law doctrine of unjust enrichment, it is inequitable for Capital One to be permitted to retain the benefits it received, and is still receiving, without justification,

from Plaintiffs and their Class and Subclass Members, and others in an unfair and unconscionable manner. Capital One's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

108. Plaintiffs, Class members, and others did not confer these benefits officiously or gratuitously, and it would be inequitable and unjust for Capital One to retain these wrongfully obtained profits.

109. Capital One is therefore liable to Plaintiffs and their Class and Subclass Members for restitution in the amount of the benefit conferred on Capital One, including Capital One's wrongfully obtained profits.

WHEREFORE, Capital One is liable to Plaintiffs and his their Class and Subclass Members for any actual damages in an amount in excess of $75,000.00 and in a sum certain amount to be determined at trial, punitive damages in an amount to be determined at trial, as well as reasonable attorney's fees, costs, and any other relief this Honorable Court deems just and proper.

A. STATE-SPECIFIC COMSUMER PROTECTION CLAIMS BROUGHT BY THE PROPOSED REPRESENTATIVES AND STATE-SPECIFIC SUBCLASSES

ALABAMA

SIXTH CLAIM FOR RELIEF

VIOLATION OF ALA. CODE §§ 8-19-1, *et seq.*
(*Asserted by Kimberly Barnes and the Alabama Subclass*)

110. Plaintiff Kimberly Barnes ("Plaintiff" for purposes of this Count), individually and on behalf of all similarly situated Alabama Subclass Members, repeats and realleges all preceding paragraphs as if fully set forth herein.

111. Capital One operating in Alabama engaged in deceptive acts and practices in the conduct of trade or commerce in violation of the Alabama Deceptive Trade Practices Act, which prohibits "(5) [r]epresenting that goods or services have sponsorship, approval, characteristics,

ingredients, uses, benefits, or qualities that they do not have," "(7) [r]epresenting that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another," and "(27) [e]ngaging in any other unconscionable, false, misleading, or deceptive act or practice in the conduct of trade or commerce," Ala. Code § 8-19-5, including but not limited to the following:

a. Failing to enact adequate privacy and security procedures and practices to protect Alabama Subclass Members' Sensitive Information from unauthorized disclosure, release, Data Breaches, and theft, which was a direct and proximate cause of the Capital One Data Breach;

b. Failing to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Capital One Data Breach;

c. Knowingly and fraudulently misrepresenting that it would maintain adequate data privacy and security practices and procedures to safeguard the Alabama Subclass Members' Sensitive Information from unauthorized disclosure, release, Data Breaches, and theft;

d. Omitting, suppressing, and concealing the material fact of the inadequacy of its privacy and security protections for the Alabama Subclass Members' Sensitive Information;

e. Knowingly and fraudulently misrepresenting that it would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the Alabama Subclass Members' Sensitive Information, including but not limited to duties imposed by the FCRA and the GLBA; and

f. Failing to maintain the privacy and security of the Alabama Subclass Members' Sensitive Information, in violation of duties imposed by applicable federal and state laws, including but not limited to those mentioned in the foregoing paragraph, directly and proximately causing the Capital One Data Breach.

112. As a direct and proximate result of Capital One's unlawful practices, Alabama Subclass Members suffered injury and/or damages, including but not limited to time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft, and loss of value of their Sensitive Information.

113. The foregoing unlawful and deceptive acts and practices by Capital One were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to the Alabama Subclass Members that they could not reasonably avoid, and this substantial injury outweighed any benefits to consumers or to competition.

114. Capital One knew or should have known that its computer systems and data security practices were inadequate to safeguard Alabama Subclass Members' Sensitive Information and that risk of a Data Breach or theft was highly likely. Capital One's actions in engaging in the abovenamed unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Alabama Subclass members.

115. Pursuant to Ala. Code § 8-19-10, Plaintiffs and the Alabama Subclass seek monetary relief against Capital One measured as the greater of (a) actual damages in an amount to be determined at trial and (b) statutory damages in the amount of $100 for each Plaintiffs and each Alabama Subclass Member.

116. Plaintiff Barnes and Alabama Subclass Members also seek an order enjoining Capital One's unfair, unlawful, and/or deceptive practices, attorneys' fees, and any other just and proper relief available under the Alabama Deceptive Trade Practices Act, Ala. Code §§ 8-19-1, *et seq*.

WHEREFORE, Capital One is liable to Plaintiff Barnes and her Subclass Members for any actual damages in an amount in excess of $75,000.00 and in a sum certain amount to be determined at trial, punitive damages in an amount to be determined at trial, as well as reasonable attorney's fees, costs, and any other relief this Honorable Court deems just and proper.

DISTRICT OF COLUMBIA

SEVENTH CLAIM FOR RELIEF

VIOLATION OF D.C. CODE § 28-3901, *et seq.*

(*Asserted by Devon Reid and the District of Columbia Subclass*)

117. Plaintiff Devon Reid ("Plaintiff" for purposes of this Count), individually and on behalf of the District of Columbia Subclass Members, repeats and realleges all preceding paragraphs as if fully set forth herein.

118. Plaintiff Reid and his District of Columbia Subclass Members entered into a transaction with Capital One primarily for personal, family, and/or household purposes and are therefore "consumers" within the meaning of D.C. Code §28-3901, *et seq.*

119. Capital One Capital One, while operating and conducting business in the District of Columbia, engaged in unlawful trade practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of goods and services in violation of D.C. Code § 28-3904, including but not limited to:

a. Misrepresenting material facts, pertaining to the sale of goods and services, to the District of Columbia Subclass by representing that it would maintain adequate data privacy and security practices and procedures to safeguard District of Columbia Subclass Members' Sensitive Information from unauthorized disclosure, release, Data Breaches, and theft in violation of D.C. Code §§ 28-3904(a), (d), (e),(f), (h), and/or (u);

b. Misrepresenting material facts, pertaining to the sale of goods and services, to the District of Columbia Subclass by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of District of Columbia Subclass Members' Sensitive Information in violation of D.C. Code §§ 28-3904(a), (d), (e), (f), (h), and/or (u);

c. Omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for District of Columbia Subclass Members' Sensitive Information in violation of D.C. Code §§ 28-3904(a), (d), (e), (f), (h), and/or (u);

d. Engaging in unfair acts and practices with respect to the sale of goods and services by failing to maintain the privacy and security of District of Columbia Subclass Members' Sensitive Information, in violation of duties imposed by and public policies reflected inapplicable federal and state laws, resulting in the Capital One Data Breach. These unfair acts and practices violated the duties imposed by laws including but not limited to the FCRA;

e. Engaging in unfair acts and practices with respect to the sale of goods and services by failing to disclose the Capital One Data Breach to District of Columbia Subclass Members in a timely and accurate manner, in violation of D.C. Code § 28-3852(a);f. Engaging in unfair acts and practices with respect to the sale of goods and services by failing to take proper action following the Capital One Data Breach to enact adequate privacy and security measures and protect District of Columbia Subclass Members' Sensitive Information from further unauthorized disclosure, release, Data Breaches, and theft.

120. The above unfair and deceptive practices and acts by Capital One were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and District of Columbia Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

121. Capital One knew or should have known that its computer systems and data security practices were inadequate to safeguard District of Columbia Subclass Members' Sensitive Information and that risk of a Data Breach or theft was high. Capital One's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the District of Columbia Subclass.

122. As a direct and proximate result of Capital One's unlawful practices, District of Columbia Subclass Members suffered injury and/or damages.

WHEREFORE, Capital One is liable to Plaintiff Reid and his Subclass Members seek relief under D.C. Code § 28-3905(k), including, but not limited to, restitution, injunctive relief, punitive damages, attorneys' fees and costs, treble damages or $1500 per violation, whichever is greater, and any other relief this Honorable Court deems just and proper.

GEORGIA

EIGHTH CLAIM FOR RELIEF

VIOLATION OF GA. CODE ANN. §10-1-370, *et seq.*

(*Asserted by Amanda Comonte and the Georgia Subclass*)

123. Plaintiff Amanda Comonte ("Plaintiff" for purposes of this Count), individually and on behalf of all similarly situated Georgia Subclass Members, repeats and realleges all preceding paragraphs as if fully set forth herein.

124. Capital One, Plaintiff, and Georgia Subclass Members are "persons" within the meaning of the Georgia Uniform Deceptive Trade Practices Act ("Georgia UDTPA"), Ga. Code Ann. § 10-1-371(5). 295. The Georgia UDTPA prohibits "deceptive trade practices," which include the "misrepresentation of standard or quality of goods or services," and "engaging in any other conduct which similarly creates a likelihood of confusion or of misunderstanding." Ga. Code Ann. § 10-1-372(a).

125. In the course of its business, Capital One willfully failed to disclose and actively concealed its grave data-security defects as discussed herein, and otherwise engaged in activities with a tendency or capacity to deceive.

126. Capital One also engaged in unlawful trade practices by employing deception, deceptive acts or practices, fraud, misrepresentations, or concealment, suppression, or omission of material facts with intent that others rely upon such concealment, suppression, or omission, in connection with accessing and storing the extremely sensitive and valuable Sensitive Information of Plaintiffs and Georgia Subclass Members.

127. Capital One did all of this directly with respect to Plaintiffs and Georgia Subclass Members, and also by way of their transactions involving goods, merchandise, and services with third parties (such as prospective creditors and creditors) who also accessed Plaintiffs and Georgia Subclass Members' extremely sensitive and valuable Sensitive Information in the course of those transactions.

128. For months, Capital One knew of vulnerabilities and defects in its data security systems, and vulnerabilities in key databases storing the extremely sensitive and valuable Sensitive Information of Plaintiffs and Georgia Subclass Members, but concealed all of that information.

129. By way of the foregoing, Capital One engaged in deceptive business practices in violation of the Georgia UDTPA.

130. Capital One also engaged in deceptive acts and practices in at least the following ways:

a. Mispresenting material facts (intending for others to rely upon the misrepresentations) representing that it would maintain adequate data privacy and security practices and procedures to safeguard Georgia Subclass Members' Sensitive Information from unauthorized disclosure, release, Data Breaches, and theft;

b. Misrepresenting material facts (intending for others to rely upon the misrepresentations) by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Georgia Subclass Members' Sensitive Information;

c. Omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Georgia Subclass Members' Sensitive Information, with the intent that others rely on the omission, suppression, and concealment;

d. Engaging in deceptive acts and practices by failing to maintain the privacy and security of Georgia Subclass Members' Sensitive Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws including but not limited to the FRCA, the GLBA, and the Ga. Code Ann. §§ 10-1-911, et seq.;

e. Engaging in deceptive acts and practices by failing to disclose the Data Breach to Georgia Subclass Members in a timely and accurate manner, in violation of Ga. Code Ann. § 10-1-912; and

f. Engaging in deceptive acts and practices by failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Georgia Subclass Members' Sensitive Information from further unauthorized disclosure, release, Data Breaches, and theft.

131. Capital One's unfair or deceptive acts or practices were likely to and did in fact deceive reasonable consumers, including Plaintiffs and Georgia Subclass Members, regarding the security and safety of its databases and the extremely sensitive and valuable Sensitive Information of Plaintiffs and Georgia Subclass Members.

132. Capital One intentionally and knowingly misrepresented such material facts with intent to mislead Plaintiffs and Georgia Subclass Members.

133. Capital One knew or should have known that its conduct violated the Georgia UDTPA.

134. As alleged above, Capital One made material statements that were either false or misleading.

135. Capital One owed Plaintiff Comonte and Georgia Subclass Members a duty to disclose the true facts regarding data-security defects and vulnerabilities because Capital One:

136. Possessed exclusive knowledge regarding the lack of safety of the extremely sensitive and valuable Sensitive Information of Plaintiffs and Georgia Subclass Members;

137. Intentionally concealed the foregoing from Plaintiffs and Georgia Subclass Members;

138. Made incomplete representations regarding these matters while purposefully withholding material facts from Plaintiffs and Georgia Subclass Members that contradicted these representations.

139. Capital One's representations and omissions were material to Plaintiffs and Georgia Subclass Members given the extreme sensitivity and value of their Sensitive Information.

140. Plaintiff Comonte and her Georgia Subclass Members suffered ascertainable loss caused by Capital One's misrepresentations and its concealment of and failure to disclose material information as alleged herein.

141. Capital One had an ongoing duty to all Capital One customers, including Plaintiff Comonte and her Georgia Subclass Members, to refrain from unfair and deceptive practices under the Georgia UDTPA.

142. Capital One's violations present a continuing risk to Plaintiff Comont and her Georgia Subclass Members, as well as to the general public.

143. Capital One's unlawful acts and practices complained of herein affect the public interest.

144. As a direct and proximate result of Capital One's violations of the Georgia UDTPA, Plaintiffs and Georgia Subclass Members have suffered injury-in-fact and/or actual damage.

WHEREFORE, Plaintiff Comonte and her Georgia Subclass Members seek an order enjoining Capital One's unfair, unlawful, and/or deceptive practices, attorneys' fees, and any other just and proper relief available under the Georgia UDTPA per Ga. Code Ann. § 10-1-373, and any further relief this Honorable Court deems just and proper.

ILLINOIS

NINETH CLAIM FOR RELIEF

VIOLATION OF THE ILLINOIS CONSUMER FRAUD ACT

(*Asserted by Michael Lewis and the Georgia Subclass*)

145. Plaintiff Michael Lewis ("Plaintiff" for purposes of this Count), individually and on behalf of all similarly situated Georgia Subclass Members, repeats and realleges all preceding paragraphs as if fully set forth herein.

146. Capital One operating in Illinois engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of 815 Ill. Comp. Stat. § 505/2, including but not limited to the following:

a. Fraudulently advertising material facts pertaining to the goods and services to Illinois Subclass Members by representing and advertising that it would maintain adequate data privacy and security practices and procedures to safeguard Illinois Subclass Members' Sensitive Information from unauthorized disclosure, release, Data Breaches, and theft;

b. Misrepresenting material facts pertaining to goods and services to Illinois Subclass Members by representing and advertising that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Illinois Subclass Members' Sensitive Information;

c. Omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Illinois Subclass Members' Sensitive Information with the intent that others rely on the omission, suppression, and concealment;

d. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Illinois Subclass Members' Sensitive Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Capital One Data Breach. These unfair acts and practices violated duties imposed by laws including but not limited to the FCRA, the GLBA, the Illinois Insurance Information and Privacy Protection Act (215 Ill. Comp. Stat. § 5/1014), Illinois laws regulating the use and disclosure of Social Security Numbers (815 Ill. Comp. Stat § 505/2RR), and the Illinois Uniform Deceptive Trade Practices Act (815 Ill. Comp. Stat. § 510/2(a));

e. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Capital One Data Breach to Illinois Subclass Members in a timely and accurate manner, contrary to the duties imposed by 815 Ill. Comp. Stat. § 530/10(a); and

f. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the Capital One Data Breach to enact adequate privacy and security measures and protect Illinois Subclass Members' Sensitive Information from further unauthorized disclosure, release, Data Breaches, and theft.

147. As a direct and proximate result of Capital One's deceptive trade practices, Illinois Subclass Members suffered injuries, including the loss of their legally protected interest in the confidentiality and privacy of their Sensitive Information, and damages, as described above.

148. The above unfair and deceptive practices and acts by Capital One were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

149. Capital One knew or should have known that its computer systems and data security practices were inadequate to safeguard Illinois Subclass Members' Sensitive Information and that risk of a Data Breach or theft was high. Capital One's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Illinois Subclass.

WHEREFORE, Plaintiffs and Illinois Subclass Members seek relief under 815 Ill. Comp. Stat. § 505/10a, including, but not limited to, damages, restitution, punitive damages, injunctive relief, and/or attorneys' fees and costs, and any other relief this Honorable Court deems just and proper.

TENTH CLAIM FOR RELIEF

VIOLATION OF 815 ILL. COMP. STAT. §§ 510/2, *et seq.*
(*Asserted by Michael Lewis and the Georgia Subclass*)

150. Plaintiff Michael Lewis ("Plaintiff" for purposes of this Count), individually and on behalf of the other Illinois Subclass Members, repeats and alleges all preceding paragraphs as if fully alleged herein.

151. While in the course of its businesses, Capital One operating in Illinois engaged in deceptive trade practices by making false representations, including its representations that it had

adequate computer systems and data security practices to protect Sensitive Information, when its computer systems and data security practices were inadequate, in violation of 815 Ill. Comp. Stat. §§ 510/2(a)(5), and (7).

152. Capital One knew or should have known that its computer systems and data security practices were inadequate and engaged in negligent, knowing, and/or willful acts of deception.

153. Illinois Subclass Members are likely to be damaged by Capital One's deceptive trade practices.

WHEREFORE, Plaintiff Lewis and Illinois Subclass Members seek relief under 815 Ill. Comp. Stat. § 510, including, but not limited to, injunctive relief and attorney's fees.

MARYLAND

ELEVENTH CLAIM FOR RELIEF
Violation of Md. Code. Ann., Com. Law §§ 13-301 *et seq.*
(*Asserted by Joseph Cook and the Maryland Subclass Members*)

154. Plaintiff ("Plaintiff" for purposes of this Count), individually and on behalf of the Maryland Subclass Members, repeats and realleges all preceding paragraphs as if fully set forth herein.

155. Plaintiffs and the Maryland Subclass Members are "consumers" within the meaning of Md. Code Ann., Com. Law §§ 13-101.

156. The goods and services that are the subject of this Complaint are "consumer goods" and/or "consumer services" as meant by Md. Code Ann., Com. Law § 13-101.

157. The unlawful trade practices, misrepresentations, and omissions described herein did not constitute "professional services" on the part of Capital One.

158. Capital One, while operating and conducting business in the Maryland, engaged in unlawful trade practices, misrepresentations, and the concealment, suppression, and omission of

material facts with respect to the sale and advertisement of goods and services in violation of Md. Code Ann., Com. Law §§ 13-301, *et seq.*, including but not limited to:

a. Misrepresenting material facts, pertaining to the sale of goods and services, to the Maryland Subclass by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Maryland Subclass Members' Sensitive Information from unauthorized disclosure, release, Data Breaches, and theft in violation of Md. Code Ann., Com. Law §§ 13-301(1), (2)(i), (2)(iv), (3), (5)(i), (9)(i), (9)(iii), and/or 14(xxi);

b. Misrepresenting material facts, pertaining to the sale of goods and services, to the Maryland Subclass by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Maryland Subclass Members' Sensitive Information in violation of Md. Code Ann., Com. Law §§ 13-301(1), (2)(i), (2)(iv), (3), (5)(i), (9)(i), (9)(iii), and/or 14(xxi);

c. Omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Maryland Subclass Members' Sensitive Information in violation of Md. Code Ann., Com. Law §§ 13-301(1), (2)(i), (2)(iv), (3), (5)(i), (9)(i), (9)(iii), and/or 14(xxi);

d. Engaging in unfair acts and practices with respect to the sale of goods and services by failing to maintain the privacy and security of Maryland Subclass Members' Sensitive Information, in violation of duties imposed by and public policies reflected inapplicable federal and state laws, resulting in the Capital One Data Breach. These unfair acts and practices violated the duties imposed by laws including but not limited to the FCRA, Maryland's Privacy of Consumer Financial and Health Information regulations (Md. Code Regs. §§ 31.16.08.01, *et seq.*);

e. Engaging in unfair acts and practices with respect to the sale of goods and services by failing to disclose the Capital One Data Breach to Maryland Subclass Members in a timely and accurate manner, in violation Md. Code Ann., Com. Law § 14-3504(b)(3); and

f. Engaging in unfair acts and practices with respect to the sale of goods and services by failing to take proper action following the Capital One Data Breach to enact adequate privacy and security measures and protect Maryland Subclass Members' Sensitive Information from further unauthorized disclosure, release, Data Breaches, and theft.

159. The above unfair and deceptive practices and acts by Capital One were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and

Maryland Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

160. Capital One knew or should have known that its computer systems and data security practices were inadequate to safeguard Maryland Subclass Members' Sensitive Information and that risk of a Data Breach or theft was high. Capital One's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Maryland Subclass.

161. As a direct and proximate result of Capital One's unlawful practices, Maryland Subclass Members suffered injury and/or damages.

162. Plaintiffs and Maryland Subclass Members seek relief under D.C. Code § 28-3905(k), including, but not limited to, restitution, injunctive relief, punitive damages, attorneys' fees and costs.

WHEREFORE, Capital One is liable to Plaintiffs and his their Class and Subclass Members for any actual damages in an amount in excess of $75,000.00 and in a sum certain amount to be determined at trial, punitive damages in an amount to be determined at trial, as well as reasonable attorney's fees, costs, and any other relief this Honorable Court deems just and proper.

NORTH CAROLINA

TWELVTH CLAIM FOR RELIEF

N.C. Gen. Stat §§ 75-1.1, *et seq.*

(*Asserted by Plaintiff Bret Glidewell and the North Carolina Subclass Members*)

163. Plaintiff Bret Glidewell ("Plaintiff" for purposes of this Count), individually and on behalf of the North Carolina Subclass Members, repeats and realleges all preceding paragraphs as if fully set forth herein.

164. Capital One's sale, advertising, and marketing of its goods and services affected commerce, as meant by N.C. Gen. Stat. Ann. § 75-1.1.

165. Capital One operating in North Carolina engaged in unlawful, unfair, and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of goods and services in violation of N.C. Gen. Stat. Ann. § 75-1.1, including but not limited to the following:

a. Misrepresenting material facts, pertaining to the sale of goods and services, to the North Carolina Subclass by representing that it would maintain adequate data privacy and security practices and procedures to safeguard North Carolina Subclass Members' Sensitive Information from unauthorized disclosure, release, Data Breaches, and theft;

b. Misrepresenting material facts, pertaining to the sale of its good and services, to the North Carolina Subclass by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of North Carolina Subclass Members' Sensitive Information;

c. Omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for North Carolina Subclass Members' Sensitive Information;

d. Engaging in unfair, unlawful, and deceptive acts and practices with respect to the sale of its goods and services by failing to maintain the privacy and security of North Carolina Subclass Members' Sensitive Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Capital One Data Breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws including but not limited to the FCRA, the GLBA, and the North Carolina Identity Theft Protection Act (N.C. Gen. Stat. Art. 2A §§ 75-60, *et seq.*);

e. Engaging in unfair, unlawful, and deceptive acts and practices with respect to the sale of goods and services by failing to disclose the Capital One Data Breach to North Carolina Subclass Members in a timely and accurate manner, in violation of N.C. Gen. Stat. Ann. § 76-65(a); and

f. Engaging in unfair, unlawful, and deceptive acts and practices with respect to the sale of its goods and services by failing to take proper action following the Capital One Data Breach to enact adequate privacy and security measures and protect North Carolina Subclass Members' Sensitive Information from further unauthorized disclosure, release, Data Breaches, and theft.

166. The above unfair, unlawful, and deceptive acts and practices by Capital One were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and North Carolina Subclass Members that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

167. Capital One knew or should have known that its computer systems and data security practices were inadequate to safeguard North Carolina Subclass Members' Sensitive Information and that risk of a Data Breach or theft was high. Capital One's actions in engaging in the abovenamed unfair, unconscionable, and deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the North Carolina Subclass.

168. As a direct and proximate result of Capital One's unfair, unconscionable, and deceptive acts and practices, North Carolina Subclass Members suffered injury and/or damages.

169. Plaintiffs and North Carolina Subclass Members seek relief under N.C. Gen. Stat. Ann. §§ 75-16 and 75-16.1, including, but not limited to, injunctive relief, actual damages, treble damages, and attorneys' fees and costs.

WHEREFORE, Capital One is liable to Plaintiffs and his their Class and Subclass Members for any actual damages in an amount in excess of $75,000.00 and in a sum certain amount to be determined at trial, punitive damages in an amount to be determined at trial, as well as reasonable attorney's fees, costs, and any other relief this Honorable Court deems just and proper.

THIRTEENTH CLAIM FOR RELIEF

VIOLATION OF N.C. GEN. STAT. ART. 2A § 75-65, *et seq.*

(*Asserted by Bret Glidewell and the North Carolina Subclass Members*)

170. Plaintiff Bret Glidewell, individually and on behalf of the North Carolina Subclass Members, repeats and realleges all preceding paragraphs as if fully set forth herein.

171. Capital One is a business that owns or licenses computerized data that includes Sensitive Information as defined by N.C. Gen. Stat. Art. 2A § 75-61(1). 447. Plaintiffs and North Carolina Subclass Members are "consumers" as defined by N.C. Gen. Stat. Art. 2A § 75-61(2).

172. Capital One is required to accurately notify Plaintiffs and North Carolina Subclass Members if it discovers a security breach or receives notice of a security breach (where unencrypted and unredacted Sensitive Information was accessed or acquired by unauthorized persons), without unreasonable delay under N.C. Gen. Stat. Art. 2A § 75-65.

173. Plaintiff's and North Carolina Subclass Members' Sensitive Information includes Sensitive Information as covered under N.C. Gen. Stat. Art. 2A § 75-61(10).

174. Because Capital One discovered a security breach and had notice of a security breach (where unencrypted and unredacted Sensitive Information was accessed or acquired by unauthorized persons), Capital One had an obligation to disclose the Capital One Data Breach in a timely and accurate fashion as mandated by N.C. Gen. Stat. Art. 2A. § 75-65.

175. As a direct and proximate result of Capital One's violations of N.C. Gen. Stat. Art. 2A § 75-65, Plaintiffs and North Carolina Subclass Members suffered damages, as above.

176. Plaintiffs and North Carolina Subclass Members seek relief under N.C. Gen. Stat. Art. 2A § 75-65, including, but not limited to, a civil fine.

WHEREFORE, Capital One is liable to Plaintiffs and his their Class and Subclass Members for any actual damages in an amount in excess of $75,000.00 and in a sum certain amount to be determined at trial, punitive damages in an amount to be determined at trial, as well as reasonable attorney's fees, costs, and any other relief this Honorable Court deems just and proper.

VIRGINIA

THIRTEENTH CLAIM FOR RELIEF

VIOLATION OF VA. CODE. ANN. §-65 59.1-196, *et seq.*
(*Asserted by David Curto and the Virginia Subclass Members*)

177. Plaintiff David Curto ("Plaintiff" for purposes of this Count), individually and on behalf of the Virginia Subclass Members, repeats and realleges all preceding paragraphs as if fully set forth herein.

178. The Virginia Consumer Protection Act prohibits "[u]sing any . . . deception, fraud, false pretense, false promise, or misrepresentation in connection with a consumer transaction." Va. Code Ann. § 59.1-200(14).

179. Capital One compiled, maintained, used, and furnished Plaintiff's and Virginia Subclass Members' Sensitive Information in connection with consumer transactions, as defined under Va. Code Ann. § 59.1-198, including, for example, credit assessments.

180. Capital One operating in Virginia engaged in deceptive trade practices in connection with consumer transactions, including by representing that its goods and services had characteristics that they did not have, representing that its services were of a particular standard or quality when they were not, and advertising its services with intent not to sell them as advertised, in violation of Va. Code Ann. § 59.1-200. This includes but is not limited to the following:

a. Failing to enact adequate privacy and security measures to protect Virginia Subclass Members' Sensitive Information from unauthorized disclosure, release, Data Breaches, and theft, which was a direct and proximate cause of the Capital One Data Breach;

b. Failing to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Capital One Data Breach;

c. Knowingly and fraudulently misrepresenting that it would maintain adequate data privacy and security practices and procedures to safeguard Virginia Subclass Members' Sensitive Information from unauthorized disclosure, release, Data Breaches, and theft;

d. Omitting, suppressing, and concealing the material fact of the inadequacy of its privacy and security protections for Virginia Subclass Members' Sensitive Information;

e. Knowingly and fraudulently misrepresenting that it would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Virginia Subclass Members' Sensitive Information, including but not limited to duties imposed by the FCRA and the GLBA; and

f. Failing to maintain the privacy and security of Virginia Subclass Members' Sensitive Information, in violation of duties imposed by applicable federal and state laws, including but not limited to those mentioned in the aforementioned paragraph, directly and proximately causing the Capital One Data Breach.

181. As a direct and proximate result of Capital One's practices, Virginia Subclass Members suffered injury and/or damages, including but not limited to time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their Sensitive Information.

182. The above unfair and deceptive acts and practices by Capital One were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Virginia Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

183. Capital One knew or should have known that its computer systems and data security practices were inadequate to safeguard Virginia Subclass Members' Sensitive Information and that risk of a Data Breach or theft was high. Capital One's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful.

184. Plaintiffs and Virginia Subclass Members seek all available relief under Va. Code Ann. § 59.1-204, including, but not limited to, actual damages, statutory damages and/or penalties in the amount of $1,000 per violation or, in the alternative, $500 per violation, restitution, injunctive relief, punitive damages, and attorneys' fees and costs.

WHEREFORE, Capital One is liable to Plaintiffs and his their Class and Subclass Members for any actual damages in an amount in excess of $75,000.00 and in a sum certain amount to be determined at trial, punitive damages in an amount to be determined at trial, as well as reasonable attorney's fees, costs, and any other relief this Honorable Court deems just and proper.

FOURTEENTH CLAIM FOR RELIEF
VIOLATION OF VA. CODE. ANN. §§ 18.2-186.6, *et seq.*
(*Asserted by David Curto and the Virginia Subclass Members*)

185. Plaintiff David Curto ("Plaintiff" for purposes of this Count), individually and on behalf of the Virginia Subclass Members, repeats and realleges all preceding paragraphs as if fully set forth herein.

186. Capital One is required to accurately notify Plaintiffs and Virginia Subclass Members following discovery or notification of a breach of its data security system (if unencrypted or unredacted Sensitive Information was or is reasonably believed to have been accessed and acquired by an unauthorized person who will, or it is reasonably believed who will, engage in identify theft or another fraud) without unreasonable delay under Va. Code Ann. § 18.2-186.6(B).

187. Capital One is an entity that owns or licenses computerized data that includes Sensitive Information as defined by Va. Code Ann. § 18.2-186.6(B).

188. Plaintiff's and Virginia Subclass Members' Sensitive Information includes Sensitive Information as covered under Va. Code Ann. § 18.2-186.6(A).

189. Because Capital One discovered a breach of its security system (in which unencrypted or unredacted Sensitive Information was or is reasonably believed to have been accessed and acquired by an unauthorized person, who will, or it is reasonably believed who will, engage in identify theft or another fraud), Capital One had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Va. Code Ann. § 18.2-186.6(B).

190. As a direct and proximate result of Capital One's violations of Va. Code Ann. § 18.2-186.6(B), Plaintiffs and Virginia Subclass Members suffered damages, as described above.

191. Plaintiffs and Virginia Subclass Members seek relief under Va. Code Ann. § 18.2-186.6(I), including, but not limited to, actual damages.

WHEREFORE, Capital One is liable to Plaintiffs and his their Class and Subclass Members for any actual damages in an amount in excess of $75,000.00 and in a sum certain amount to be determined at trial, punitive damages in an amount to be determined at trial, as well as reasonable attorney's fees, costs, and any other relief this Honorable Court deems just and proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of their Class and Subclass Members, respectfully pray that this Court enter judgment in their favor, and further:

a. Certify of the Class and Subclasses;

b. Appoint Plaintiffs as Class and Subclass representatives;

c. Appoint Michael A. Yoder, Esq., Michael W. Slocumb, Esq. and Scott A. Powell, Esq. as Class counsel;

d. Award Plaintiffs and members of the Class and Subclasses compensatory damages in excess of $5,000,000.00;

e. Award Plaintiffs and proposed Class and Subclass Members of the Class and Subclasses punitive damages in an amount to be determined at trial;

f. Award Plaintiffs and proposed Class and Subclass members Subclasses equitable, injunctive, and declaratory relief, including enjoining Capital One's unlawful business practices from continuation any further as a consequence of Capital Ones' inadequate data protection practices, protocols, and procedures;

g. Declare Capital Ones' acts and omissions regarding Defendants' data protection practices, protocols, and procedures are negligent;

h. Award Plaintiffs and proposed Class and Subclass members both pre and post-judgment interest at the highest legal rate until paid in full;

i. Award Plaintiffs and proposed Class and Subclass members reasonable attorney's fees and costs; and

j. Award Plaintiffs and proposed Class and Subclass members any other relief this Honorable Court deems just and proper.

Dated: August 6, 2019

Respectfully submitted,

KIMBERLY BARNES, DEVON REID, AMANDA COMONOTE, MICHAEL LEWIS, CRYSTAL BIGGS, BRET GLIDEWELL, and JOSEPH COOK, individually, and on behalf of all others similarly situated

/S/ MICHAEL A. YODER
Michael A. Yoder, Esquire [VSB 93863]
SLOCUMB LAW FIRM, LLC
777 6th Street NW, Suite 520
Washington, D.C. 20001
Tel: (202) 737-4141
Fax: (202) 710-9933
myoder@slocumblaw.com
Local Counsel

/S/ MICHAEL W. SLOCUMB
Michael W. Slocumb, Esquire
SLOCUMB LAW FIRM, LLC
777 6th Street NW, Suite 520
Washington, D.C. 20001
Tel: (202) 737-4141
Fax: (202) 710-9933
mike@slocumblaw.com
*Pro Hac Vice pending**

/S/ SCOTT A. POWELL
Scott A. Powell, Esquire
HARE, WYNN, NEWELL & NEWTON, LLP
2025 Third Avenue North, 8th Floor
Birmingham, Alabama 35203
Tel: (205) 328-5330
Fax: (205) 324-2165
scott@hwnn.com
*Pro Hac Vice pending**

COUNSEL FOR PLAINTIFFS

JURY DEMAND

Plaintiffs, individually and on behalf of all similarly situated individuals and proposed Class and Subclass Members demand a trial by jury on all issues so triable pursuant to FED. R. CIV. P. 38.

/S/ MICHAEL A. YODER
Michael A. Yoder, Esquire